Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1741 10/30/15

~ EmuTOS 0.9.5 Released! ~ People Are Talking! ~ Aranym - Atari/OS X!
~ CISA Gets Less Popular ~ Secure Password, $2.00 ~ Tor Private IM Tool!
~ TalkTalk Hack Arrest! ~ EU Net Neutrality Vote ~ Firebee News Update!

~ FinFisher Use Rampant! ~ SXSW Turns Tail, Runs! ~ Goodbye Other Inbox!

-* cOS Released for Commodore 64 *-
-* Dragon’s Lair Non-interactive Movie *-
-* Call for More Robust Privacy Legislation! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
"""""""""""""""""""""""""""""

Happy Halloween! Yes, it’s that fun time of the year when little kids roam the neighborhood streets all dressed up in their various scary (and not-so-scary) costumes, "threatening" everyone with a trick unless provided a handful of candy treats! I guess we’ll soon find out how we’re going to fare this year; I plan to stock up on candy in the morning (and hope that we manage to have some extra)! I may be too old to join in on the festivities, but never too old to give up my sweet tooth!

So, please be extra safe driving this weekend, avoiding all of the little ghosts and goblins walking in the streets going from house to house seeking treats. Experience shows us that there will be a lot of costumed-kids that will be difficult to see once the sun sets. We don’t want to spoil anyone’s fun by driving carelessly!

Until next time...

=~=~=~=

EmuTOS 0.9.5 Released

Dear FreeMiNT users,

EmuTOS 0.9.5 has been released.

The main features are:
- AES/BIOS: implement critical error handler
- BDOS: implement Pexec mode 7
- BIOS: add alt-arrow support (mouse actions via keyboard)
- BIOS: add dual keyboard support (for Greek/Russian keyboards)
- BIOS: allow user to specify boot partition at startup
- BIOS: allow EmuTOS to recover from program exceptions in user programs
- BIOS: auto-detect multiple IDE interfaces
- EmuDesk: improve text object alignment for translated strings
- VDI: add line-A flood fill; all line-A opcodes are now supported

You can download your preferred binary archive there:
http://sourceforge.net/projects/emutos/files/emutos/0.9.5/

Enjoy!

Roger Burrows

Dear FireBee users,

EmuTOS 0.9.5 has just been released.

It includes some fixes specifically for the FireBee and other
Coldfire systems:
- AES: increase AES stack size for Coldfire machines
        this allows programs using USERDEFs and GEMLIB (such as
        QED) to run natively on EmuTOS
- BIOS: add explicit delay for parallel port strobe
        this allows programs to print via the parallel port on
        the FireBee the latest version of the FPGA is also
        required)

FireBee users can also benefit from other major features of this
release,
including:
- AES/BIOS: implement critical error handler
- BIOS: allow user to specify boot partition at startup
- BIOS: allow EmuTOS to recover from program exceptions in user
  programs
- BIOS: auto-detect multiple IDE interfaces
- EmuDesk: improve text object alignment for translated strings

Get EmuTOS 0.9.5 here:
http://sourceforge.net/projects/emutos/files/emutos/0.9.5/

Download emutos-firebee-0.9.5.zip, then flash emutosfb.s19 with
your preferred tool.

Enjoy!

Roger Burrows

Aranym-user - ATARI/OS X

Hi,

ARAnyM (http://aranym.org) is the ATARI GNU/GPL virtual machine.
The *miniPack* which is a minimal configuration of ARAnyM, is
updated with the new 0.9.5 version of EmuTOS. It runs on
Macintosh:

http://eureka.atari.org/miniPack.zip

The v.1.0.2 of the ‘MacAranym JIT‘ application runs from OS X
Leopard (10.5) up to OS X El Capitan (10.11).

Here is a screenshot http://eureka.atari.org/aranym.gif

Comments are welcome. Enjoy, this is yours =)

--
Francois Le Coat
Author of Eureka 2.12 (2D Graph Describer, 3D Modeller)
http://eureka.atari.org

cOS Has Been Released for the Commodore 64!

This project started as a simple experiment to see if I could create a "modern" looking graphical user interface for the commodore 64.

Once I got the basic user interface working, I decided to add an optional touch screen. It pretty much works! Of course cOS can still be operated by a standard joystick or the cursor keys.

I then decided to create a Test / Demo 5.25" disk that would have a similar feel as a basic tablet. I ended up adding pictures, songs, games, and some typical iPad style apps. These disks only hold 170k of data! So, I used a 80's disk notcher to make a "flippy" 2-sided disk. I then had a whopping 340k of space to fill up.

The iPad style apps are mostly gags for fun. Yes, there are real internet programs for the commodore 64 (IRC clients, twitter client, contiki web browser, etc.) but they are typically large and require specific hardware. Who could resist Microsoft's insistence that I include IE 6 (running on Windows 9)! There's also a cBooks app that links to all the books you'll need. Of course these devices need a sassy assistant. I pulled together some 80's technology to create SAM-Siri.

If you have a real commodore 64 or want to try it out in an emulator, here are links to the disk images for sides A and B of the Test/Demo disk.

Disk Links:
cOS Test/Demo Side A
https://drive.google.com/file/d/0B65J_0YDdJyITUU0QkxlMmJHeTQ/view
cOS Test/Demo Side B
https://drive.google.com/file/d/0B65J_0YDdJyIZEx6QlJDc0JTb00/view

FireBee News Update

by Fred Horvat

Not a whole lot to report this week with my use of the FireBee. I did go through the process of update much of the firmware (FPGA, FireTOS, EmuTOS, and BaS GCC) on the FireBee. There was some excitement but I am back up and running again. I'm slightly better off after upgrading the FPGA firmware as the

annoying keyboard bugs appeared to have finally gone away. I still can not run some supported software (Netsurf 3.4) still on the FireBee but I am still not done testing things out to know why yet. I did not try EasyMiNT 1.90 after updating the firmware but will again soon. To read the whole adventure you can go here: http://www.atari-forum.com/viewtopic.php?f=92&t=28704

=~=~=~=

->In This Week's Gaming Section - Dragon s Lair Non-Interactive Movie?
"""""""""""""""""""""""""""""""""

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""""""

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

Dragon s Lair Gets A Kickstarter To Pitch A Non-Interactive Movie

I saw this spreading around all over the place yesterday so I m not exactly hot on the press with it but no worries. This stuff always takes a back seat to new arcade games or new arcade locations??

So yes, there is a Kickstarter to turn the arcade classic Dragon s Lair into a bona-fide, non-interactive movie. It should be noted that the Kickstarter isn t to develop the movie itself but to develop the pitch which is needed to potentially turn it into a bigger budget movie. Here is a long video with Don Bluth and Gary Goldman talking about various projects, including their ideas for the official DL movie:

Granted, it is a little surprising that this has taken such a long time to come to fruition, especially where the Dragon s Lair game has been ported to everything that can handle interactive video, including Blu-Ray players and phones. For the record, my first experience with the game was actually on the Atari Jaguar CD console; in the arcade I ve only come across and played

Dragon s Lair II since most original DL cabinets find themselves in private collections as opposed to on location.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

CISA: Why Tech Leaders Hate the Latest Cyber-Security Bill

A bill called the Cybersecurity Information Sharing Act CISA for short has become one of the least popular tech-policy proposals since another would-be law with a four-letter acronym became a four-letter word in tech circles.

CISA is no SOPA (the controversial Stop Online Piracy Act from a few years back, which would have empowered copyright holders to order allegedly infringing sites off the map of the Internet). But many tech leaders have lined up against CISA as if it were the spawn of SOPA.

For instance, Apple condemned CISA in a statement to the Washington Post: The trust of our customers means everything to us and we don t believe security should come at the expense of their privacy.

Twitter backed away from the bill in a tweet from its public-policy account: Security+privacy are both priorities for us and therefore we can t support #CISA as written.

Not to be left out, NSA whistleblower Edward Snowden has been denouncing the proposal on Twitter as the zombie #CISA surveillance bill.

And yet the Senate seems likely to pass its version of CISA (it goes by the bill number S.754) after considering a series of amendments to it Tuesday, and President Obama seems likely to sign it into law. What is it about this bill that has techies so on edge?

The basic point of CISA is to make it easier for companies to share information about online threats with each other and with government authorities.

It s not a new or crazy idea: Versions of this bill have been coming up for years. That s because the history of companies trying to engage hackers in solo or semi-solo combat is not encouraging.

As the Edison Electric Institute, a trade group of power utilities, said in a recent statement: The sharing of information needs to be faster, more actionable, and more

efficient. To support these efforts, companies need more structure and legal certainty.

(Security professionals don t all buy that logic. Many organizations do successfully share data among themselves and with government entities [e.g. law enforcement] in formal and informal ways, emailed Johannes Ullrich, a researcher who runs a clearinghouse of threats called the Internet Storm Center.)

The question is, how do you provide that legal support while also keeping customers personal information private?

Supporters of CISA say it achieves that balance by requiring companies that volunteer to share threat information with the Department of Homeland Security to strip out personal information of or identifying a specific person not directly related to a cybersecurity threat before handing it over.

Opponents say that phrasing isn t strong enough and also object to CISA s notwithstanding any other provision of law grant of immunity to corporations that share threat info.

4-letter bill, 3-letter agency

What really sets off CISA foes, however, is the bill s requirement that threat reports be shared in an automated manner with all of the appropriate Federal entities.

That list of seven entities includes the Office of the Director of National Intelligence which, in turn, means the National Security Agency. Yes, Snowden s favorite three-letter agency, the one his disclosures revealed had been conducting widespread domestic surveillance.

Summed up Greg Nojeim, senior counsel with the Center for Democracy and Technology: CISA permits companies to share information directly with the NSA, notwithstanding any law.

This is where the debate about CISA broadens to a more existential issue: Do you trust the government?

It s one on which there is no obvious left/right split: Sen. Ron Wyden, D.-Ore., doesn t like this bill and neither does his Republican/libertarian colleague from Kentucky, GOP presidential candidate Rand Paul.

Conversely, not all of Big Tech hates the bill. Earlier in October, IBM said CISA would affirmatively advance the cause of privacy because it would help defend against hacking attempts that often end in the massive disclosure of personal information.

How do you solve CISA?

Tuesday s votes on a series of proposed CISA amendments may ease the concerns of CISA skeptics or leave them angrier about the bill.

Nojeim, for instance, said he wants to see the Senate pass Wyden s amendment requiring more thorough scrubbing of personal data before any sharing of threats; it would limit the damage this bill could do.

But Mozilla public-policy head Chris Riley said none of the possible amendments would fix CISA enough that we feel the bill is worth passing. The Electronic Frontier Foundation came to the same conclusion weeks ago, condemning CISA for its vague definitions, broad legal immunity, and new spying powers.

If CISA does pass, I can promise that two things won t change.

One is that far longer-running tech privacy and security problems will remain unsolved, thanks to congressional inaction. The Computer Fraud and Abuse Act s wide-open definitions will continue to threaten legitimate security research, and the Electronic Communications Privacy Act will offer pathetically little protection of messages stored online.

The other is that companies and government offices will continue to expose your data not because they didn t communicate with competitors or the government, but because they didn t listen to warnings from their own employees about insecure systems. As a look at some of Congress s other work ought to remind anybody, you can t outlaw stupidity.

Call For Robust Privacy Legislation In Wake Of EU Safe Harbor Strike-Down

A group of U.S. and EU digital rights organizations and consumer NGOs including the EFF, the U.S. Center for Digital Democracy, the European Consumer Organization and Privacy International have issued a statement calling for a meaningful legal framework to protect fundamental privacy rights in the digital era.

The statement comes as a critical response to the publication earlier this month of the Bridges report: a joint project between U.S. and EU academics and including the involvement of the Dutch data protection agency advocating for continued reliance on existing laws coupled with industry self-regulation as a middle-of-the-road approach to safeguarding privacy rights.

The Bridges report advocates for, as they put it, a framework of practical options that advance strong, globally-accepted privacy values in a manner that respects the substantive and procedural differences between the two jurisdictions such as offering standardized user controls and user complaint mechanisms, and best practices for the de-identification of user data, among other proposed measures.

However the EFF et al are highly critical of this approach dubbing it failed policy and remarkably out of touch with the current legal reality .

 Digital rights organization and consumer NGOs call on the Data Protection Commissioners to refocus their attention on the need to update and enforce privacy law, the group said today.

The current legal reality on the U.S.-EU data privacy front includes the ruling, earlier this month, by Europe s top court, the ECJ, invalidating the Safe Harbor data-sharing agreement

which had governed data flows between the regions for some 15 years, allowing companies sending EU data to the U.S. for processing to self-certify they would provide adequate protection .

The court ruled that such self-certification failed in an era of mass surveillance by government intelligence agency dragnets opening the door to individual reviews of data transfers by data protection authorities in individual European Member States.

This is not a situation conducive to operational certainty for businesses with DPAs already issuing differing opinions on the current post-Safe Harbor scenario. For example, guidance issued by the U.K. s ICO differs greatly in tone from a position paper published by German data supervisory authorities in the wake of the ECJ ruling.

So while the ICO is telling businesses and organizations not to panic or rush to other transfer mechanisms that may turn out to be less than ideal arguing the impact of the judgement is still being analysed the German DPAs suggest they will immediately be prohibiting data transfers to the U.S. that are solely based on Safe Harbor, as well as specifying other explicit controls, such as that consent clauses cannot be used to sanction repeated, mass or routine data transfers .

Meanwhile, the European Commission is attempting to hammer out a so-called Safe Harbor 2.0 agreement with the U.S. in the next few weeks, to try to reestablish a data flows agreement. Although any such deal is likely to face fresh legal challenges unless the U.S. agrees to substantial concessions on surveillance and privacy rights. (Yet only yesterday the Senate passed another bill that critics say will expand government agencies surveillance capabilities)

With existing legal frameworks governing data protection under continued pressure from the surveillance state and new tech challenges to privacy pushing into the frame all the time, whether it s from AI-powered big data processing or drone surveillance the EFF et al are pressing the case for a comprehensive privacy legal framework to offer robust consumer protection, and ultimately also create legal certainty for businesses.

Particularly after the Safe Harbor decision, the Bridges report is remarkably out of touch with the current legal reality and what we need to do to address it, they write, criticizing the report for failing to recommend any substantive changes in law .

The practical consequence of focusing instead on failed policies, such as self regulation, will be to make more difficult the work of the privacy experts around the world who could have otherwise benefitted from a meaningful discussion about how to move forward on legislation, aggressive enforcement, and other steps that are long overdue. Yes, they are difficult; all the more reason why we need to act now, they add.

Updates: Responding to criticism of the Bridges report and approach, Daniel Weitzner, one of the project participants and

director of MIT s Cybersecurity and Internet Policy Research Initiative, said the aim is not to encourage industry self-regulation but rather to call on the FTC and European data protection authorities to engage in collaborative policy development .

He also stressed that the call for the development of better user control technologies is something the report says can only happen with clear guidelines and legal interpretations from regulators .

 We re not saying industry should set rules through design (that would be self-regulation) but rather that policy guidance from governments is vital, said Weitzner.

 We do hope that we can contribute to progress on legislative development in both the US and EU, he added. I myself spent about three years working in the Obama Administration toward issuing and trying to get the US Congress to pass the Consumer Privacy Bill of Rights. That remains very important to me, but I m also pursuing other avenues for progress.

Net Neutrality: EU Votes in Favour of Internet Fast Lanes and Slow Lanes

The European Parliament has passed the flawed compromise text on net neutrality without including any of the amendments that would have closed serious loopholes. The vote, with 500 in favour, and 163 against, took place in a plenary session a few hours after a rather lacklustre debate this morning, which was attended by only 50 MEPs out of the European Parliament’s total of 751, indicating little interest in this key topic among most European politicians. The Greens MEP Jan Philipp Albrecht called the final result a "dirty deal."

Arguments in favour of the text were disappointing and superficial. Many concentrated on the other major component of the Telecoms Single Market package, the abolition of mobile roaming charges in the EU. This long-overdue, and highly-popular measure was cleverly offered as a carrot by the Council of the EU and the European Commission in order to persuade MEPs to accept the rest of the package. The misleading impression was given that supporting the net neutrality amendments proposed by MEPs would cause the abolition of roaming charges to be lost, but that was not the case.

As the German Pirate Party MEP Julia Reda pointed out, the Telecoms Single Market package doesn’t even deliver on roaming: "The plan to place an end to roaming surcharges in Europe has been adopted pending a review of pricing and consumption patterns. Even if the review is completed by the 15 June 2017 deadline, roaming surcharges will only be suspended up to a fair use limit beyond which they still apply and continue to hinder the breaking down of barriers within Europe." In other words, those MEPs who voted in favour of the package in the belief that accepting poor net neutrality rules was a price worth paying in order to buy a speedy end to EU roaming charges were played for mugs.

On the few occasions that MEPs supporting the compromise text addressed the net neutrality rules directly, they simply parroted the claim by telecom companies that specialised services running over fast lanes were needed in order to encourage innovation in the EU. As those in favour of true net neutrality including such luminaries as Sir Tim Berners-Lee have emphasised, the opposite is true. For innovation to flourish as it has done so far, a level playing-field is needed. Allowing fast and slow lanes on the Internet plays into the hands of incumbents and companies with deep pockets.

Pressure was applied at the end of the morning’s debate by Andrus Ansip, the vice-commissioner responsible for the EU Digital Market. He said that if the text was not passed in its entirety now, there was "a risk of delays, not only months, but years," and that "risk" may have weighed with some MEPs. But Reda pointed out on Twitter that is not true: "Actually it’s only 6 weeks until 3rd reading," when a new compromise text could have been agreed. One other reason MEPs may have been unwilling to change the text was that it has been going back and forth between the various institutions of the EU for years, and MEPs are evidently sick of discussing it, as the poor turn-out for the earlier debate showed. In the end, sheer political fatigue may have played a major part in undermining net neutrality in the EU.

However, the battle is not quite over. As Anne Jellema, CEO of the Web Foundation, which was established by Berners-Lee in 2009, notes in her response to today’s EU vote: "The European Parliament is essentially tossing a hot potato to the Body of European Regulators, national regulators and the courts, who will have to decide how these spectacularly unclear rules will be implemented. The onus is now on these groups to heed the call of hundreds of thousands of concerned citizens and prevent a two-speed Internet."

Arrest Made in TalkTalk Hacking Case

A teenager in Northern Ireland suspected of playing a part in the cyberattack on British telco TalkTalk Telecom Group PLC has been arrested, police here said Monday.

The development is the first major breakthrough in the case, opened Oct. 22 after a significant and sustained breach of TalkTalk s website that the company said could have resulted in the loss of millions of customers personal data.

Detectives from the Metropolitan Police s specialist cybercrime unit arrested the unnamed 15-year-old boy on suspicion of breaking the U.K. s Computer Misuse Act shortly after 4 p.m. local time, the police said in a statement.

Officers from the cybercrime unit and the Northern Irish police force continued to search a property in County Antrim for evidence late Monday, said the police.

The suspect remains in custody and is being questioned. In the

U.K., criminal suspects aren t named before formal charges are laid, though even if the teen is charged with a criminal offense, he is unlikely to be named by authorities due to laws designed to protect underage offenders.

The TalkTalk hack is the latest in a series of cyberattacks on the company. In February, TalkTalk said criminals breached its security systems internally and obtained customers personal data by impersonating sales staff. In August, it said external criminals obtained data by attacking the computer servers of high-street cellphone retailer Carphone Warehouse.

On Monday, TalkTalk said it was grateful for the swift response and hard work of the police. We will continue to assist with the ongoing investigation.

An Alarming Number of Governments Are Using FinFisher Malware

According to a study carried out by the Citizen Lab (a research department at the University of Toronto), FinFisher is the most used spyware by many government agencies around the world.

Finfisher was developed by a German security company (FinFisher GmBH). The company has been selling this spyware to many law enforcement agencies from many different parts of the world.

FinFisher used in the past for illegal government surveillance:

This spyware is used illegally because it s been sold to only law enforcements agencies in many states like Ethiopia and Bahrain have been found using the Spyware illegally. States like these have been using this spyware as a way of keeping the people who oppose the state s policies quiet.

Spyware s way of working:

The spyware has a complete system by which it transfers all the information from the spied PC to the agencies. It all starts from the spyware picking up the information from the PC then sending data to a C&C server through proxies.

This works nearly the same way Tor system works but minus the complex encryptions.

Citizen lab, in the past, were unable to differentiate the FinFisher replays and C&C server, but they are now able to differentiate and also many FinFisher network all around the world.

FinFisher spyware infrastructure:

According to Citizen Lab, FinFisher has reached 32 countries so far. 135 instances of the spyware have been observed (Including both the replays and servers).

Among the mentioned countries, Pakistan was the only one where civil society challenged the use of Finfisher spyware in the

court.

Furthermore, Citizen Lab was also able to trace the IP addresses of C&C servers which belonged to 10 different agencies. What s even worse is that the relay servers of different countries are located in other countries, which can allow one country s agency to look into another s.

The market for intrusion software like FinFisher is challenging to track because the key players, from government customers to software developers, have a strong interest in keeping transactions private, say the Citizen Lab researchers.

2014 data breach helped the company gain more deals:

FinFisher GmBH was hacked in 2014 and some 40 GB data from the company was leaked. But, it wasn t enough to find useful stuff regarding the widespread use of their spyware.

But, interestingly, it did increase the demand for the spyware as more countries demand for spying increase with each passing day. Wikileaks document also referred to this in its recent leaks.

SXSW Turns Tail and Runs, Nixing Panels on Harassment

Threats of violence have led the popular South by Southwest (SXSW) festival to nix two panel discussions about online harassment, organizers announced on Monday.

In his post, SXSW Interactive Director Hugh Forrest didn’t go into detail about the threats.

But given the names of the panels cancelled, there’s a strong smell of #gamergate in the air.

Namely, the panels for the 2016 event, announced about a week ago, were titled "SavePoint: A Discussion on the Gaming Community" and "Level Up: Overcoming Harassment in Games."

This reaction sure isn’t what they had in mind, Forrest wrote:

> We had hoped that hosting these two discussions in March 2016 in Austin would lead to a valuable exchange of ideas on this very important topic.
>
> However, in the seven days since announcing these two sessions, SXSW has received numerous threats of on-site violence related to this programming. SXSW prides itself on being a big tent and a marketplace of diverse people and diverse ideas.
>
> However, preserving the sanctity of the big tent at SXSW Interactive necessitates that we keep the dialogue civil and respectful.

Arthur Chu, who was going to be a male ally on the Level Up panel, has written up the behind-the-scenes mayhem for The Daily

Beast.

As Chu tells it, SXSW has a process of making proposed panels available for - disastrously enough, given the tactics of torch-bearing villagers - a public vote.

Chu:

> The ability to "downvote" or "dislike" something has proven in the past to be a pretty terrible idea that, despite the best intentions of implementers, serves to encourage mobs of haters to go after unpopular people and suppress them, and is a major reason why places like Reddit become such unpleasant, polarized echo chambers.
>
> Speaking of Reddit: Once SXSW s "PanelPicker" website went live, three panels got targeted by r/KotakuInAction, a subreddit that serves as a primary GamerGate discussion forum ours, a panel called "Level Up: Overcoming Harassment In Games," and a panel about VR technology that was apparently targeted simply because Brianna Wu was on it.

Brianna Wu is a US-based game developer who was one of multiple women involved in gamergate who were slated to be on the panels.

At any rate, beyond the subsequent brigading of downvoters, there were also the comments.

Oh, the comments.

SXSW was aware of them, Chu says, but initially refused to close down the unmoderated comment section left on each PanelPicker page:

> I asked that a link to a hit piece alleging over-the-top and incredibly hurtful things about a panelist that she was a drug addict, and that she d sold her child be removed. I asked that a link to a hit piece saying I'd called in a bomb threat be removed. I asked that a link outing the birth name of a trans person who wasn't even on any of the panels be removed.

His requests were ignored, Chu said. It was only when one of the panelists spoke up about having her mother be swatted were the comments closed.

The story goes on, and Wu has called Chu's piece an accurate description of it.

While SXSW organizers are protecting the "sanctity" of their big tent, others are feeling like they've suddenly been thrust out of the tent completely, even if their panel was focused on online harassment in general, not gamergate in particular.

Online Abuse Prevention Initiative's Randi Harper, who would have been one of the panelists:

The ripples haven't stopped spreading on this one.

On Wednesday, BuzzFeed announced that it would withdraw from SXSW over the canceled panels.

BuzzFeed published a letter it sent to the organizers of the Austin-based media festival on Tuesday.

From the letter:

> Digital harassment of activists of all political stripes, journalists, and women in those fields or participating in virtually any other form of digital speech has emerged as an urgent challenge for the tech companies for whom your conference is an important forum. Those targets of harassment, who include our journalists, do important work in spite of these threats.
>
> We will feel compelled to withdraw... if the conference can't find a way to do what those other targets of harassment do every day - to carry on important conversations in the face of harassment.

Some are saying that SXSW's decision to cancel panels on online harassment shows exactly why such discussions are needed.

Others are saying that the cancellations show that SXSW can't guarantee security at its event.

Tor Releases Private IM Tool - Here's An Idiot's Guide To Using Encrypted Messaging

The Tor Project announced an instant messaging tool today, Tor Messenger.

Though not perfect, it s ideal for anyone looking for an IM tool designed with privacy in mind, as it not only encrypts communications, but routes users through the Tor network, made up of different hops or relays, to hide their original IP addresses. Logging is disabled by default too, so there should be no record of conversations.

Most web users aren t, of course, au fait with the nitty gritty of cryptographic communications. But it s now remarkably straightforward to set up encrypted instant messaging and not too tricky to do so with a good degree of security.

Here s a quick guide to downloading and using Tor Messenger securely, one that could be applied to your IM app of choice:

There are a whole host of IM services out there, but the most popular amongst security-minded folk are Jabber and Google Talk.

I use Jabber (get me at tfoxbrewster@jabber.hot-chilli.net), which is based on the XMPP messaging protocol and requires users to sign up to a server. This is a straightforward process but there are a bewildering array of options out there. Fortunately, this website rates them on their level of security by checking the connections between servers and PCs, ensuring as far as it can that there aren t any weak or broken encryption mechanisms in use. It s up to you, but I d opt for one with an A rating, such as jabber.de.

You ll now want to register an account on your chosen server. Search Google for the name of the server and registration and head to the related site. For jabber.de it s all in German, but it s not exactly hard to figure out what is required to sign up just a username and a password. Make sure the password is as secure as you can make it ideally long with a mix of upper and lowercase letters, some numbers and other characters. If there s an option to include an email address, feel free to add it, but if really concerned about privacy, use a disposable email address or just don t add one at all.
Recommended by Forbes

Register and that s that, your XMPP account is ready to use. Make sure you have a record of the account name.

For Google Talk, you ll need to register a Google account if you haven t already. Once you ve done that, you re ready to roll. Tor Messenger also supports Facebook FB -1.96% Chat that works in a similar manner in terms of sign up and use.

But how do you actually use Tor Messenger with those accounts?

Head to to the Tor website serving the download. There are various instructions for how to download depending on your operating system, but it s not very different from downloading and using a typical application from the web (though on Mac OS X, you ll have to go into the security section on System Preferences and allow the use of Tor Messenger for whatever reason, it s not trusted by Apple AAPL +0.00% Gatekeeper).

If you really want as close to 100 per cent trust in the client, you ll want to validate the files are legitimate. These checks guarantee that the download comes from the Tor Project, not some snoop or crook who has somehow managed to alter the file.

This is a little more technical, but here goes: You can check the file hasn t been tampered with by first downloading the sha256sums.txt file provided by Tor (right click, save as). This includes what is known as a hash , the result of the original file being put through an algorithm, and is unique to that file. So, if the file has been tampered with, it will have a different hash to the legitimate, trusted one. Therefore, the user can put the download through the algorithm and if it delivers the same hash as that provided by Tor, it s highly likely the app is legitimate. The result will look something like de4b6a6949b9408384f3bfe8c1fa0e4688569ca4f0eda95ae03d0829d2c695af .

As a Mac user, I d advise anyone who is happy running Terminal to follow this guide from the Apache Foundation and switch in the right files. The command I typed openssl dgst -sha256 TorMessenger-0.1.0b2-osx64_en-US.dmg and the results can be seen below:

Using Mac OS X Terminal, it s easy to quickly get the hash of a file. That can then be checked against a hash provided by those providing the file. Mine matched huzzah!

For Windows, the same link provides some good guidance. I haven t been able to find a decent app that makes this process really

simple. For instance, HashCheck is a great little app for Mac and Windows but doesn t support the SHA-256 algorithm used by the Tor Project.

Remember, this validation is great, but you re reliant on the hash files being legitimate too. The Tor Project has signed the hash file with an encryption key. For those who want to make this final check, you ll need to download GnuPGP, as well as the key provided by Tor, and then do some command line checks. I won t go into too much detail here, as the Tor Project has a great guide on how to do this. As proof that any idiot can do it, here s an example of my own signature verification:

Signature verification is the last step in verifying a file s integrity. It s not as painful as it sounds.

Do all this and you can be fairly happy you ve downloaded a safe IM client and can get cracking with actually using the thing.

Once you ve got Tor Messenger up and running, you ll be asked to add an account. For Jabber, select XMPP. Your username will be the first half of the account name you ve been given i.e. the example in example@jabber.de . The domain will be whatever server you chose i.e. the jabber.de in example@jabber.de . Click through and enter your chosen password. You should now be online.

For Google, just use the credentials you registered with. Anyone who uses two-factor authentication for their Google account (as you should if you want to be secure), can follow the process for authorising specific apps and Google will provide a one-time password to login.

Now, go and get some friends to sign up so you can start chatting. Once you initiate a conversation, Tor Messenger has a little padlock toggle. Hit that and you ll send a request for private chat. You ll then be advised to verify the contact easily done with a question, the answer for which should be known only to this contact and not some imposter. You can select a shared secret too, or rely on fingerprints cryptographically-generated, unique identifiers for the encryption keys you re using. Now get talking, hopefully, without government spies or criminal snoops watching over you.

Tor Messenger security check

Make sure the answer to your question could only be known to the person on the other end of the line.

Two final notes. First, keep an eye out for updates from the Tor Project. Like all software, it ll have vulnerabilities that hackers can exploit to spy on your conversations, so expect patches to be released frequently. Download the latest version whenever it s ready.

Lastly, keep in mind Tor s app is in beta and therefore might not be as stable or as secure as one would hope. Total security is, as always, a pipe dream.

11-Year-old Sells Secure Passwords Online for Two Bucks

Online security is a bigger concern now that it ever has been, as our passwords control access to everything from personal email correspondence to our bank accounts. A good password is worth its weight in gold but an entrepreneurial 11-year-old from New York City will supply you with one for just two dollars. Sixth grader Mira Modi uses the Diceware system to create secure passwords for her customers. By rolling standard six-sided dice, she comes up with random numbers that correspond to different words. When those words are combined into a string, they re difficult for a computer to crack, but easy for humans to remember. Modi has managed to sell thirty passwords in her first month of business, according to Ars Technica. Despite the nature of the endeavor, her process is pleasingly low-tech; she rolls real-world dice, looks up the matching words on a physical copy of the Diceware word list and then handwrites the resulting password to be distributed via snail mail.

Is a safe password even possible? We ask an expert The project was inspired by Modi s mother, tech journalist and author Julia Angwin. During the research process for a recent book, Angwin tasked her daughter with some Diceware work upon completing the task, Modi realized that there might be some spending money on the table if she could sell to the right consumers. Modi initially sold her passwords to attendees at the various book events that she was taken to by her mother. However, business wasn t quite as vigorous as she would have liked, so she s now attempting to corner the online market with an online store. The business sense displayed by the 11-year-old Modi is commendable but keeping one eye on the world of online security is perhaps even more impressive. Privacy concerns will only become more of an issue in the years to come, so it s encouraging to see good password habits being promoted with a fun project such as this.

Online security is a bigger concern now that it ever has been, as our passwords control access to everything from personal email correspondence to our bank accounts. A good password is worth its weight in gold but an entrepreneurial 11-year-old from New York City will supply you with one for just two dollars.

Sixth grader Mira Modi uses the Diceware system to create secure passwords for her customers. By rolling standard six-sided dice, she comes up with random numbers that correspond to different words. When those words are combined into a string, they re difficult for a computer to crack, but easy for humans to remember.

Modi has managed to sell thirty passwords in her first month of business, according to Ars Technica. Despite the nature of the endeavor, her process is pleasingly low-tech; she rolls real-world dice, looks up the matching words on a physical copy of the Diceware word list and then handwrites the resulting password to be distributed via snail mail.

The project was inspired by Modi s mother, tech journalist and author Julia Angwin. During the research process for a recent book, Angwin tasked her daughter with some Diceware work upon completing the task, Modi realized that there might be some

spending money on the table if she could sell to the right consumers.

Modi initially sold her passwords to attendees at the various book events that she was taken to by her mother. However, business wasn t quite as vigorous as she would have liked, so she s now attempting to corner the online market with an online store.

The business sense displayed by the 11-year-old Modi is commendable but keeping one eye on the world of online security is perhaps even more impressive. Privacy concerns will only become more of an issue in the years to come, so it s encouraging to see good password habits being promoted with a fun project such as this.

Facebook Says Goodbye To The Other Inbox

The social network announced that it will phase out the Other inbox in a few days time.

Facebook users currently receive messages from people they are not friends with in the Other inbox, but that will soon change. The move has seen a mixed reaction from users.

Among the chief concerns is that harassment and spam messages will be more visible. Under the new system, messages from non-contacts will arrive as requests which the user can choose to see or not.

According to Kleinman many users are not aware of the existence of the second inbox, which can only be accessed from Facebook via a browser. However now that all messages from unknown people will be sent as requests, they will arrive on the smartphone apps.

This will aid communication between members of public Facebook groups, where some messages sometimes get lost in the Other folder. Rebecca Smith owns a group for British bloggers, and thinks that the move will help administrators get in touch with new members.

 It means our messages won t be missed and people can t claim that they haven t been spoken to, she added. Some people keep doing the same things over and over again that we ve asked them not to because the messages we send go into their others inbox that they don t check.

After the change was announced by David Marcus, Facebook s vice president of messaging products, other users raised concerns about harassment. This means women will get creepy messages directly in their inbox. They used to be able to ignore them as they went to the others folder, wrote one.

 We truly want to make Messenger the place where you can find and privately connect with anyone you need to reach, but only be reached by the people you want to communicate with, said Mr Marcus. Now, the only thing you need to talk to virtually anyone

in the world, is their name.

For some users that might not necessarily be a good thing, although they can still choose to ignore the Message Requests that they receive. Facebook continues to update its platform, but some changes are proving more popular than others.

Surface Book Suffers from Launch Day Bugs

Within hours of Microsoft's new Surface Book landing in the hands of customers I began seeing reports of serious bugs and issues affecting Microsoft's new flagship device.

While many are happy with their new purchase, there is no shortage of tales of woe. And the bugs are many and varied, and solutions for most of these - other than wait or send the machine back to Microsoft for replacement or refund - are thin on the ground.

Note that Microsoft doesn't seem to have set up an official support forum for the Surface Book as of yet, so many of these reports are coming via third-party sources.

Here are some of the issues affecting the Surface Book as reported by new owners:

- Dead on arrival (or badly limping on arrival) Surface Books
- Random crashes and lockups
- Surface Book systems working fine until they're updated, following which they fail to load
- Surface Book systems failing to boot when in the dock
- Detaching the Surface Book from the dock results in an error (the most common being related to SearchUI)
- Weird screen color temperature issue when scrolling web pages
- Random display driver errors displayed every 10 to 20 minutes
- Random trackpad freezes

There are also shortcomings related to the hardware itself:

- Problems physically connecting/disconnecting the dock, with some users ending up with the screen half-disconnected
- A screen wobble due to a weight imbalance between the screen and keyboard
- No ambient light sensor controlling the brightness of the backlit keys, something that most laptops - especially premium models - have these days
- No quad-core CPU option for those wanting more power
- Concerns about the strength of the hinge

Bugs are normal early on in a product's lifecycle, and I'm sure that many of these issues will be sorted out over the coming months. Remember also that the Surface Book is a new class of device, so you're also getting to experience all those first-gen bugs and issue.

However, for some of those who put down a few thousand dollars of their hard-earned cash to be one of the first to own a Surface

Book, the experience has been far from smooth.

Several people have asked me whether I'm considering buying a Surface Book since I'm in the market for a mobile Windows-based system for a number of projects I have on the go. The answer is "no," and that's down to the fact that I try my best to avoid first-generation hardware if at all possible because, well, I find that I end up having to spend too much time nursing it as opposed to just using it.

This Website Tells You All The People Who Have Died in Your House and Whether They Were Murdered

As Halloween approaches, there are a lot of ways you can get in the holiday season. You can carve a pumpkin, for example, or make a scarecrow or find out whether someone was ever murdered in your house.

DiedInHouse.com is a website that does exactly what you d think: it tells you whether someone ever died in your house. The site was founded in 2013 by software engineer Roy Condrey after some tenants in a house he owned asked if he knew the house was haunted, according to Forbes.

DiedInHouse.com works by searching data from death certificates, news reports, and 130 million police records to determine first whether someone died in your house, and then more specifically whether there have been any underground meth labs on the property, arson, or murders.

These spooky findings can have real implications for your house value. A death or incident of violent crime in your house can cause its value to sink up to 30%, according to Forbes.

This could present a serious problem, unless you live in an insane housing market like San Francisco, where a house in which a mummified woman had been discovered fetched $1.56 million $500,000 over asking.

We tried out three searches on the service, which starts at $11.99 (3 searches cost $19.99). None of our houses came back with dead people in its past, but Forbes had checked it against known dens of death and it passed the test. They found that it correctly identified a (former) meth lab and the Amityville Horror House.

Condrey told Forbes that the site has sold over 40,000 reports to date to a mixture of ghost hunters and concerned citizens.

If you are worried about prior deaths in a house you are looking to buy, you should check your state laws regarding disclosures, which vary widely.

Check out the website for yourself.

=~=~=~=